

SISTEM KEAMANAN E-VOTING MENGGUNAKAN ALGORITMA KODE ASCII

Prima Cop¹, Rachmat Adi Purnama²

Abstract— Conventional ballot is the voting process and to make important decisions for several parties involved. But voting is very time consuming and very tiring to wait for the results of voting. e-voting is an alternative voting process which can make easier and faster and can reduce the error rate. But the application of e-voting remains a matter of information security-related issues, namely the integrity of the data, confidentiality and availability of information. Encryption can be used to answer questions related to information security in the form of confidentiality, integrity of data, non-repudiation, and authentication. In this study, it is described how a algorithm ASCII Code is used to improve the security of information in the e-voting. The results of this study is an e-voting system using a web-based programming language PHP and Oracle database. It is shown whether the ASCII Code algorithm used is safe enough for security of information on e-voting.

Key Word: Encryption, Information Security, E-Voting.

Pemungutan suara secara konvensional atau voting adalah proses pemungutan suara dan aspirasi serta keputusan penting untuk beberapa pihak. Tetapi pemungutan secara konvensional membutuhkan waktu yang lama dan sangat melelahkan untuk menunggu hasil voting. *e-voting* menjadi alternatif proses pemungutan suara yang lebih mudah dan cepat serta dapat menurunkan tingkat kesalahan. Tetapi penerapan *e-voting* menyisakan persoalan terkait soal keamanan informasi yaitu keutuhan data (*integrity*), kerahasiaan informasi (*confidentiality*), dan ketersediaan informasi (*availability*). Enkripsi dapat dimanfaatkan untuk menjawab pertanyaan terkait dengan keamanan informasi berupa kerahasiaan, keutuhan data, nir penyangkalan, serta otentikasi. Pada skripsi ini dijelaskan bagaimana algoritma kode ASCII yaitu algoritma ASCII digunakan untuk meningkatkan keamanan informasi dalam *e-voting*. Hasil dari penelitian ini adalah sebuah sistem *e-voting* berbasis web menggunakan bahasa pemrograman PHP dan database Oracle dan menunjukkan bahwa algoritma kode ASCII cukup aman digunakan untuk keamanan informasi pada *e-voting*.

Kata Kunci: Enkripsi, Keamanan Informasi, *E-voting*.

I. PENDAHULUAN

Voting telah menjadi salah satu metode untuk mengambil keputusan penting dalam kehidupan manusia. voting digunakan mulai dari tingkat masyarakat terkecil, yaitu keluarga, sampai dengan sebuah negara. voting digunakan untuk menghimpun aspirasi dari seluruh elemen masyarakat, dan kemudian menemukan jalan keluar yang dianggap paling baik untuk menyelesaikan permasalahan. voting memiliki banyak tipe pelaksanaan, menjelaskan mengenai tipe-tipe pelaksanaan voting dan ilustrasi pelaksanaannya. Dalam negara yang menganut sistem politik demokrasi, voting digunakan untuk mengambil keputusan negara yang sangat krusial, antara lain adalah untuk memilih wakil-wakil rakyat, atau untuk memilih pemimpin negara yang baru. Akan tetapi, tidak seluruh warga negara dapat memberikan suara mereka dalam voting. Terdapat beberapa persyaratan yang harus dipenuhi oleh warga negara tersebut untuk mendapatkan haknya, dan negara wajib untuk melindungi warga negara tersebut dalam memberikan suaranya. Oleh karena itu, voting membutuhkan prosedur pelaksanaan yang dapat menjamin kerahasiaan dan keabsahan dari hasil pelaksanaan voting tersebut.

Salah satu cara yang cukup mudah dan efisien dalam pembangunan aplikasi *e-voting* pemilihan adalah dengan menggunakan arsitektur client-server. Sistem ini menjadi sebuah implementasi yang lazim dalam jaringan komputer. Ada beberapa metode arsitektur lain misalnya peer-to-peer dan client-queueclient, tetapi metode arsitektur client-server memiliki lebih banyak keunggulan, satu diantaranya adalah kemudahan dalam pengorganisasian data dan informasi. Jadi penggunaan all-computer-based voting system diharapkan mampu menekan biaya pengeluaran dalam proses voting. “Melakukan pengacakan data dan kriptografi pada data *e-voting* merupakan cara untuk menghindari terjadinya pencurian data ataupun manipulasi data *e-voting*”[4].

Maksud dari penelitian ini adalah:

1. Mengurangi kecurangan, mengamankan data dengan tingkat keamanan yang cukup tinggi, serta mengurangi biaya operasional *voting*.
2. Pemberian sistem verifikasi login dan pertanyaan keamanan serta enkripsi data yang diharapkan mampu mengamankan sistem voting berbasis web.

¹. Program Studi Sistem Informasi STMIK Nusa Mandiri Jakarta, Jln. Damai No.8 Warung Jati Barat Jakarta Selatan Telp: 021-78839513; e-mail: primacop@yahoo.com

² Program Studi Manajemen Informatika AMIK BSI Jakarta, Jl. RS Fatmawati no 24 Jakarta Selatan, Telp. 021-75914760 email : rachmat.rap@bsi.ac.id

II. KAJIAN LITERATUR

Sistem adalah suatu kumpulan atau himpunan dari unsur atau variable-variabel yang saling terorganisasi, saling berintraksi dan saling bergantung satu sama lain [2].

Pengertian dari *Electronic Voting (E-Voting)* secara umum adalah penggunaan teknologi komputer pada pelaksanaan voting. Menjelaskan secara umum sejarah, jenis *e-voting*, keuntungan dan kerugian dalam penggunaannya. Pemilihan teknologi yang digunakan dalam implementasi *e-voting* sangat bervariasi. Penerapan *e-voting* telah berjalan di beberapa Negara di benua Eropa dan Amerika.

Menurut Adnan "Bagian ini mendiskusikan rancangan *e-voting* dengan teknik pemrograman sekuensial dan juga dengan teknik pemrograman parallel multithreading". [1]

Enkripsi adalah metode transformasi sebuah pesan teks ke bentuk lain yang tidak dapat dimengerti siapapun, kecuali mereka yang memiliki kunci tertentu (disebut *key*) untuk melakukan deskripsi atau mengembalikan pesan ke bentuk semula [5]. Enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, namun hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi. Untuk menampilkan enkripsi dan kebalikannya dekripsi, digunakan algoritma yang biasa disebut *Cipher* dengan menggunakan metode serangkaian langkah yang terdefinisi yang diikuti sebagai prosedur. Alternatif lain ialah *Encipherment*. Informasi yang asli disebut sebagai *plaintext*, dan bentuk yang sudah dienkripsi disebut sebagai *chiphertext*. Pesan *chiphertext* berisi seluruh informasi dari pesan *plaintext*, tetapi tidak dalam format yang didapat dibaca manusia ataupun komputer tanpa menggunakan mekanisme yang tepat untuk melakukan dekripsi. Sedangkan Dekripsi yaitu kebalikan dari proses enkripsi yaitu proses konversi data yang sudah dienkripsi (*chiphertext*) kembali menjadi data aslinya (*Original Plaintext*) sehingga dapat dibaca/ dimengerti kembali

E-Voting (Electronic voting) adalah "proses pemilihan umum yang memungkinkan pemilih untuk mencatatkan pilihannya yang bersifat rahasia secara elektronik yang teraman".

Beberapa perangkat pendukung dalam penelitian ini antara lain :

UML merupakan bahasa visual untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung. Unified Modeling Language (UML) adalah sebuah "bahasa" yang telah menjadi standard industri untuk visualisasi, merancang dan mendokumentasikan sistem piranti lunak.[3]. Dengan menggunakan UML kita dapat membuat model untuk semua jenis aplikasi piranti lunak, dimana aplikasi tersebut dapat berjalan pada piranti keras, sistem operasi dan jaringan apapun serta ditulis dalam bahasa pemrograman apapun. Di dalam UML penulis menggunakan lima diagram diantaranya use case diagram, activity diagram, sequential diagram dan deployment diagram [6]. Adapun fungsi masing-masing diagram sebagai berikut :

1. Deployment diagram atau diagram deployment menunjukkan konfigurasi komponen dalam proses eksekusi aplikasi
2. Use case diagram merupakan pemodelan untuk kelakuan (behavior) sistem informasi yang akan dibuat
3. Activity diagram menggambarkan workflow (aliran kerja) atau aktifitas dari sebuah sistem atau proses bisnis atau menu yang ada pada perangkat lunak .
4. Sequence diagram menggambarkan kelakuan objek pada use case dengan mendeskripsikan waktu hidup objek dan message yang dikirimkan dan diterima antar objek.

Perangkat pendukung yang lain adalah flowchart, dimana Flowchart adalah penggambaran secara grafik dari langkah-langkah dan urutan-urutan prosedur suatu program [7].

III.METODE PENELITIAN

Metode penelitian yang digunakan antara lain :

1. Pengamatan (*observation*), yaitu aktivitas yang dilakukan secara cerdas, dengan maksud merasakan dan kemudian memahami yang terkandung berdasarkan ilmu pengetahuan dan gagasan yang ada sebelumnya.
2. Wawancara (*interview*), yaitu percakapan antara dua orang atau lebih untuk menggali informasi dari orang yang diwawancarai berdasarkan materi dan pertanyaan yang telah disediakan sebelumnya.
3. Riset Pustaka (*library research*), yaitu metode pengumpulan data dengan cara membaca buku-buku atau dokumen-dokumen referensi yang ada hubungannya dengan masalah yang sedang diteliti yang isinya relevan

IV.HASIL DAN PEMBAHASAN

Penggunaan internet yang sangat rentan dengan gangguan dari luar. Muncul dugaan bahwa dapat terjadi perubahan data hasil pemungutan suara. Untuk itu, penggunaan algoritma enkripsi dalam *e-Voting* mulai dianjurkan. Salah satunya, yang menerangkan algoritma enkripsi yang sebaiknya digunakan dalam proses pengiriman data hasil pemungutan suara dalam *e-Voting*.

Sering terjadinya suara ganda, data tidak aman, manipulasi suara, serta biaya *voting* manual yang mahal sehingga penulis membuat alternatif pemecahan masalah tersebut dengan membangun sistem *Electronic Voting (E-Voting)* dengan sistem keamanan yang cukup mampu untuk menghindari permasalahan *Boot* yang dilakukan mesin untuk menggandakan suara, serta membuat enkripsi pada database, serta membuat audit history sehingga aktivitas administrator dapat direkam, dan adanya sistem *e-voting* ini diharapkan mampu menekan biaya anggaran untuk melakukan *Voting*.

Permasalahan yang akan diteliti dalam pembuatan sistem keamanan *e-voting* adalah bagaimana cara membuat sistem *Voting* berbasis web yang aman, serta bagaimana cara mengontrol sistem *voting* agar tidak terjadi pemberian suara ganda dan kecurangan.

Dengan menggunakan kode ASCII (*American Standard Code for Information Interchange*) mampu untuk

memberikan keamanan data yang falid dan meminimalisir kecurangan dan suara ganda pada proses *e-voting*.

A. Analisa Kebutuhan

Kebutuhan proses dalam sistem keamanan e-voting antara lain:

1. Penentuan calon pemilih.
2. Pembatasan suara ganda.
3. Mengamankan informasi agar tidak dapat dibaca.
4. Mengantisipasi adanya manipulasi data.

B. Design

Algoritma Pada kasus

1. Enkripsi

Algoritma akan mencetak code ASCII dari huruf dari kata yang telah diinputkan, dan jika hasil ASCII huruf dari kata tersebut memiliki panjang code ASCII 2 maka akan di cetak angka "0" di depan dua code ASCII tersebut.

Jika diinputkan kata misal "prima" hasil ASCII dari huruf – huruf nya adalah sebagai berikut :

- p = 112 (panjang 3 karakter)
- r = 114 (panjang 3 karakter)
- i = 105 (panjang 3 karakter)
- m = 109 (panjang 3 karakter)
- a = 97 (panjang 2 karakter)

Huruf a panjang setelah di konversi ke ASCII menjadi "97" panjangnya 2 karakter maka ditambah angka "0" di depan angka "97" menjadi "097" maka hasil inputan "farid" akan menghasilkan output "112114105109097".

2. Dekripsi

Algoritma akan menghitung 3 karakter ASCII atau hasil enkripsi dari algoritma sebelumnya dan mengkonversikan ke karakter semula.setelah selesai hit awal akan di tambah 3 yang dimaksudkan untuk mengkonversi 3 karakter berikutnya dan seterusnya. Misal, inputan "112114105109097" :

112 (panjang 3 karakter) = p

114 (panjang 3 karakter) = r

105 (panjang 3 karakter) = i

109 (panjang 3 karakter) = m

97 (panjang 3 karakter) = a -> dimana angka "0" di depan akan di abaikan

Dan menghasilkan output "prima".

3. Audit.

Semua perubahan data dan data yang dihapus telah di rekam oleh table audit dimana table audit bertujuan sebagai history yang merekam data lama dan mengadopsi sistem TRIGGER dari ORACLE.

TRIGGER akan merekam aktifitas *update* dan *delete* pada data master yang perlu untuk dijaga keamanannya dan disimpan pada tabel audit.

Tabel audit memiliki 2 field yaitu:

a. Tanggal

Digunakan untuk merekam tanggal perubahan data oleh user.

b. Data_lama

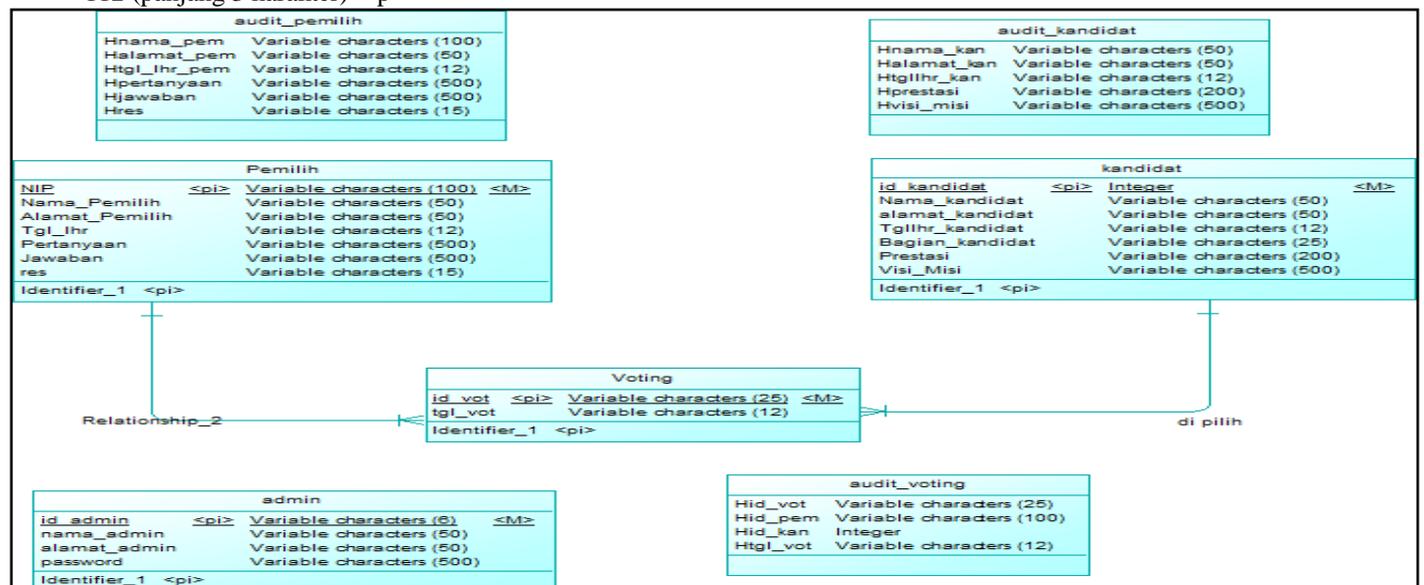
Digunakan untuk merekam data sebelum di rubah pada data master yang menggunakan fungsi "old" (lama) pada TRIGGER yang terkait dengan table – table yang mengalami perubahan.

C. Data Base

Penggunaan ORACLE sebagai 86 system database di program ini bertujuan untuk 86system keamanan data yang memanfaatkan fitur-fitur dari ORACLE yang mana akan merekam data penting yang 86yist dirubah melalui fitur admin dan di simpan dalam 86yste audit yang secara sengaja akan tidak di tampilkan dalam aplikasi ini. Berikut rancangan database 86system ini.

1. Conceptual Data Model (CDM)

Berikut adalah *Conceptual Data Model (CDM)* dari 86system ini:

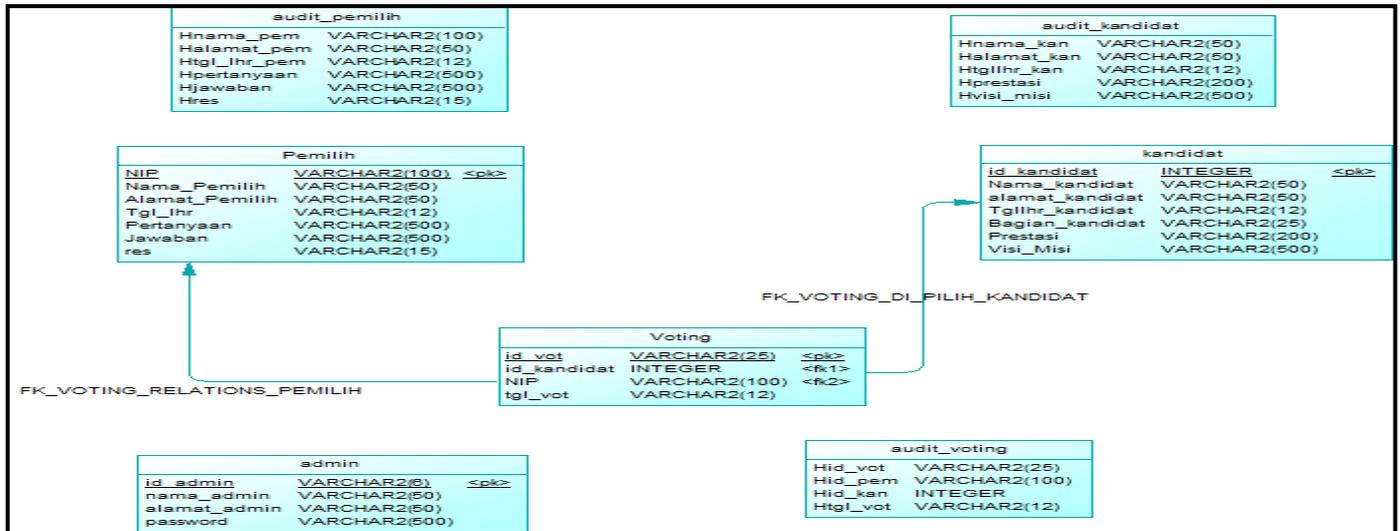


Sumber : Hasil penelitian (2014)

Gambar 1. Conceptual Data Model (CDM) e-voting

2. Physical Data Model (PDM)

Physical Data Model (PDM) adalah hasil dari generate dari Conceptual Data Model (CDM). Berikut adalah PDM dari CDM yang telah sebelumnya di buat.



Sumber : Hasil penelitian (2014)

Gambar 2. Physical Data Model (PDM) e-voting

D. Software Architecture.

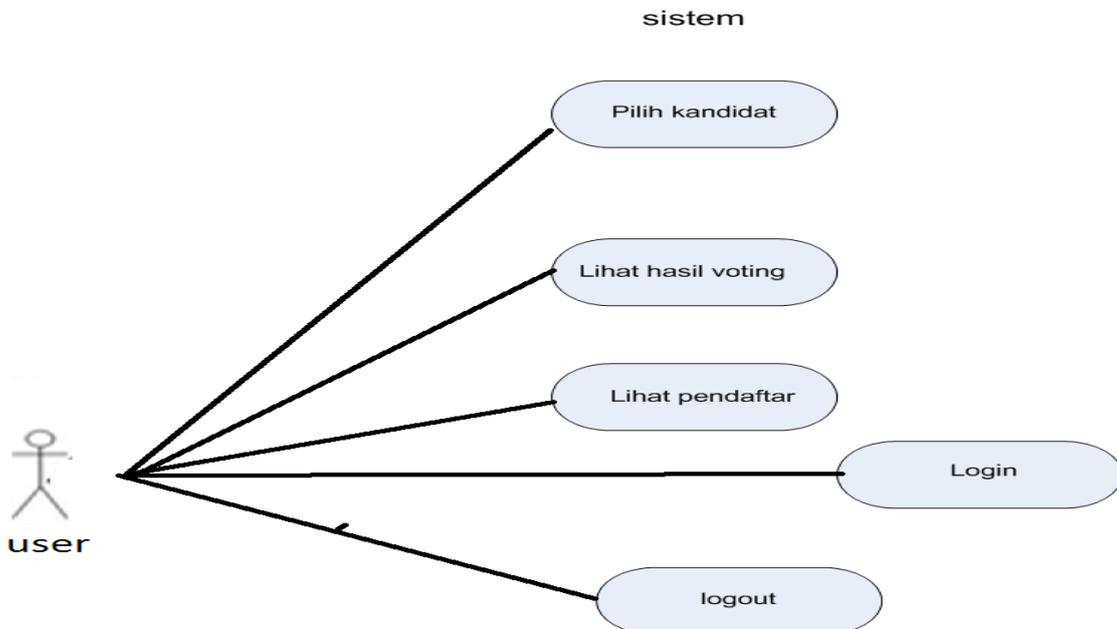
Pada sistem ini pemodelan kebutuhan fungsional dimodelkan menggunakan diagram use case. Diagram use case merupakan diagram yang memodelkan aspek perilaku sistem. Masing-masing diagram use case memiliki aktor, use case, dan hubungannya.

a. Diagram Use Case User.

Pada sistem voting ini aktor dibagi menjadi tiga bagian: administrator, dan user. User merupakan pengguna yang telah terdaftar di dalam sistem, Administrator sistem merupakan aktor yang mempunyai hak akses paling tinggi, untuk mengedit kandidat, membuat operator baru untuk pendaftaran, mengatur hasil voting.

1. Use case

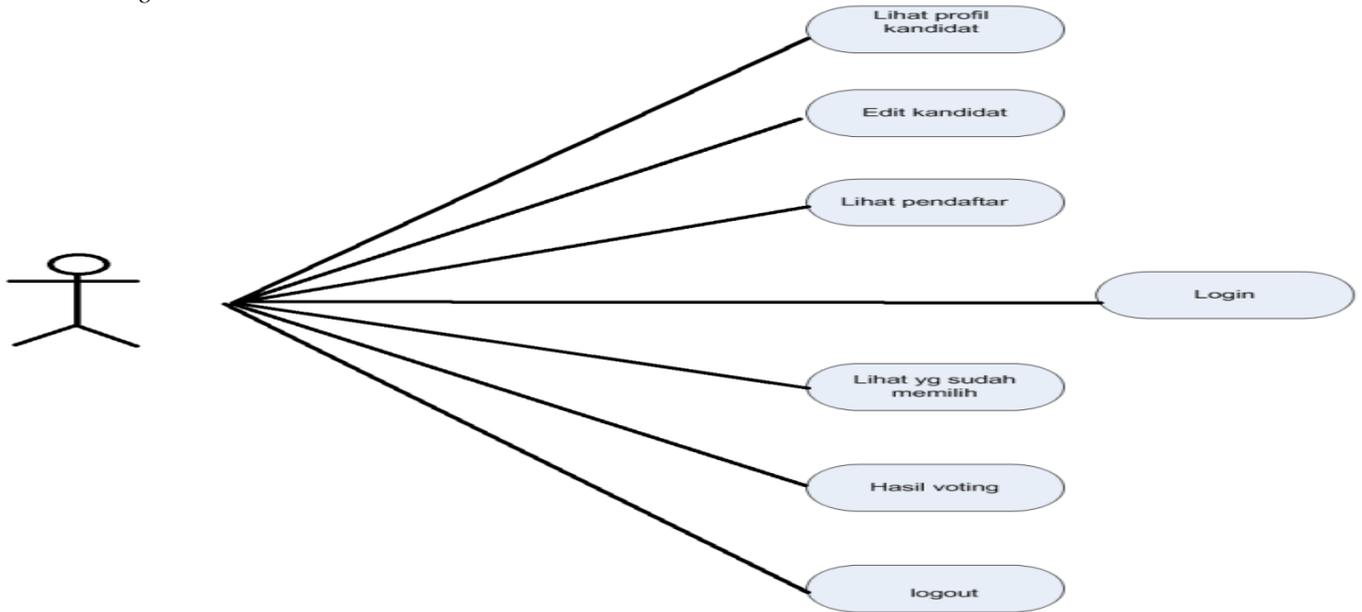
Berikut diagram use case dari masing-masing aktor.



Sumber : Hasil penelitian (2014)

Gambar 3. Use Case Diagram User

b. *Diagram Use Case Administrator.*



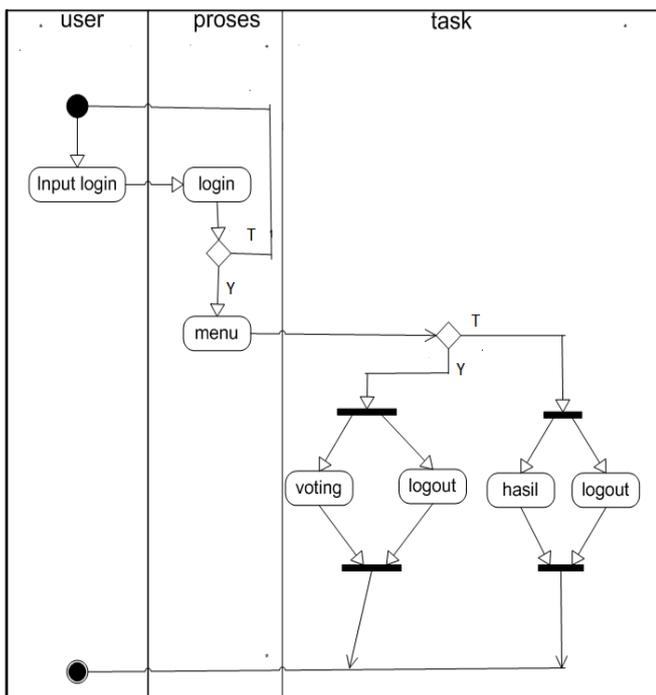
Sumber : Hasil penelitian (2014)

Gambar 4. Use Case Diagram Administrator

2. *Activity Diagram*

Untuk menggambarkan berbagai alir aktivitas dalam sistem yang sedang berjalan maka dibuatlah suatu activity diagram (diagram aktivitas). Berikut merupakan diagram aktivitas dari sistem e-voting:

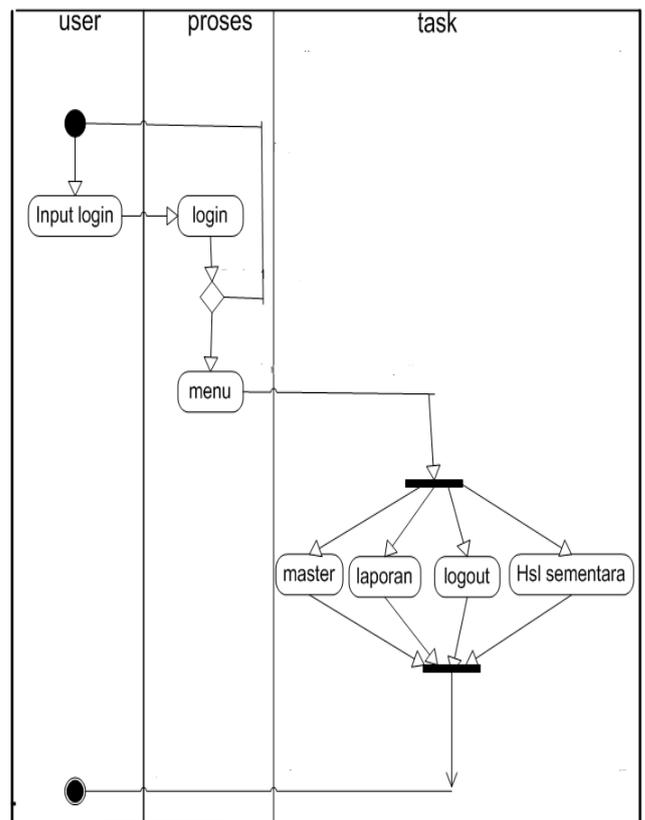
a. *Activity Diagram User.*



Sumber : Hasil penelitian (2014)

Gambar 5. Activity Diagram User

b. *Activity Diagram Administrator.*



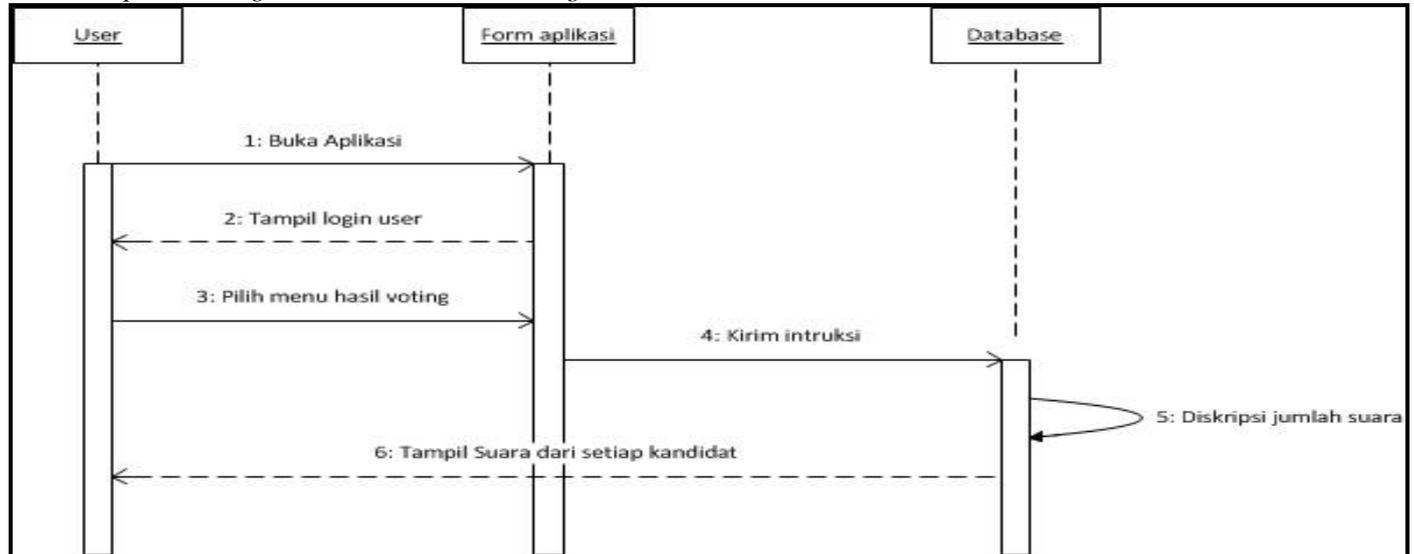
Sumber : Hasil penelitian (2014)

Gambar .6. Use Case Diagram Administrator

3. *Seqences Diagram*

Berikut merupakan diagram sequence yang menggambarkan interaksi antar objek di dalam dan sekitar sistem:

a. *Squences Diagram User: Lihat Hasil Voting*



Sumber : Hasil penelitian (2014)

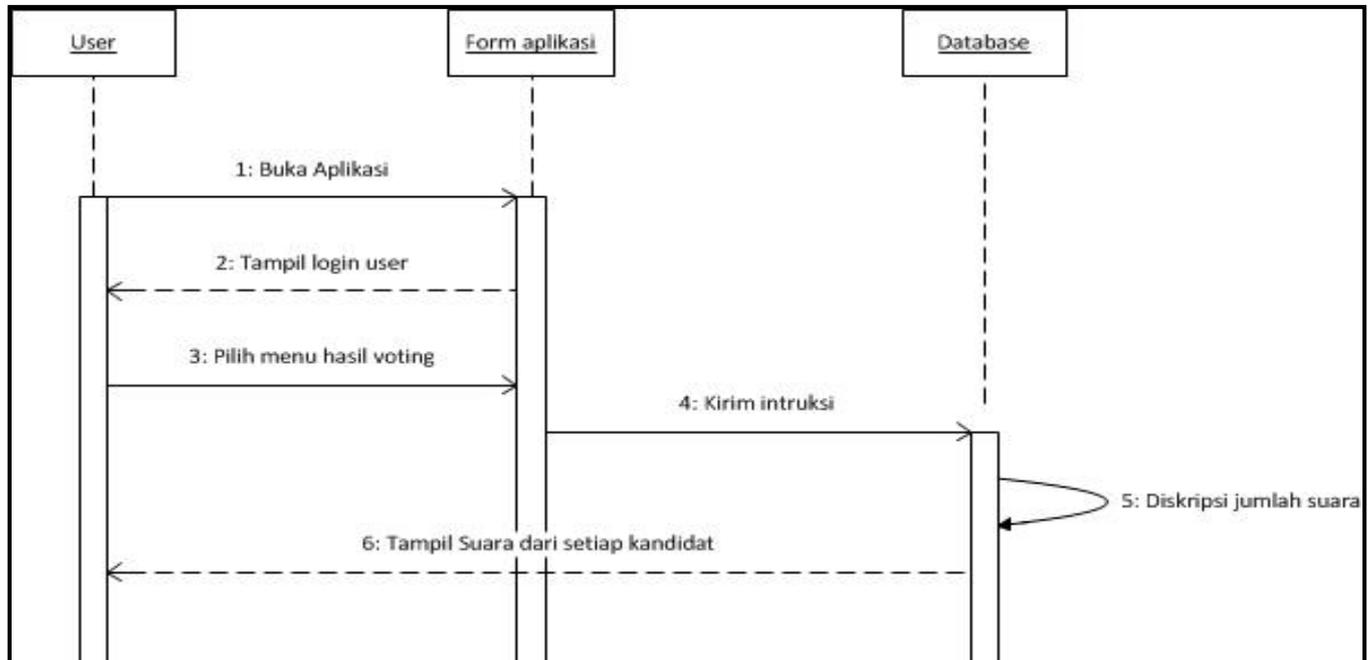
Gambar 7. *Seqence Diagram User* Lihat Hasil Voting

b. *Squences Diagram user: Pilih kandidat.*

Diagram sequence user pilih kandidat menggambarkan perilaku sistem dalam melakukan proses pilih kandidat. Sequence dimulai ketika user sign in ke dalam sistem, sistem akan memverifikasi username dan

Diagram sequence user lihat hasil voting menggambarkan perilaku sistem dalam melakukan proses menunjukkan hasil voting. Sequence dimulai ketika user memilih lihat hasil voting pada menu utama.

password yang telah diberikan. Kemudian user memilih salah satu kandidat yang ditampilkan di halaman utama user. Kemudian mengisi jawaban pertanyaan keamanan, jika benar proses pemilihan selesai, jika salah kembali ke pemilihan. Berikut *Seqences Diagram* nya:

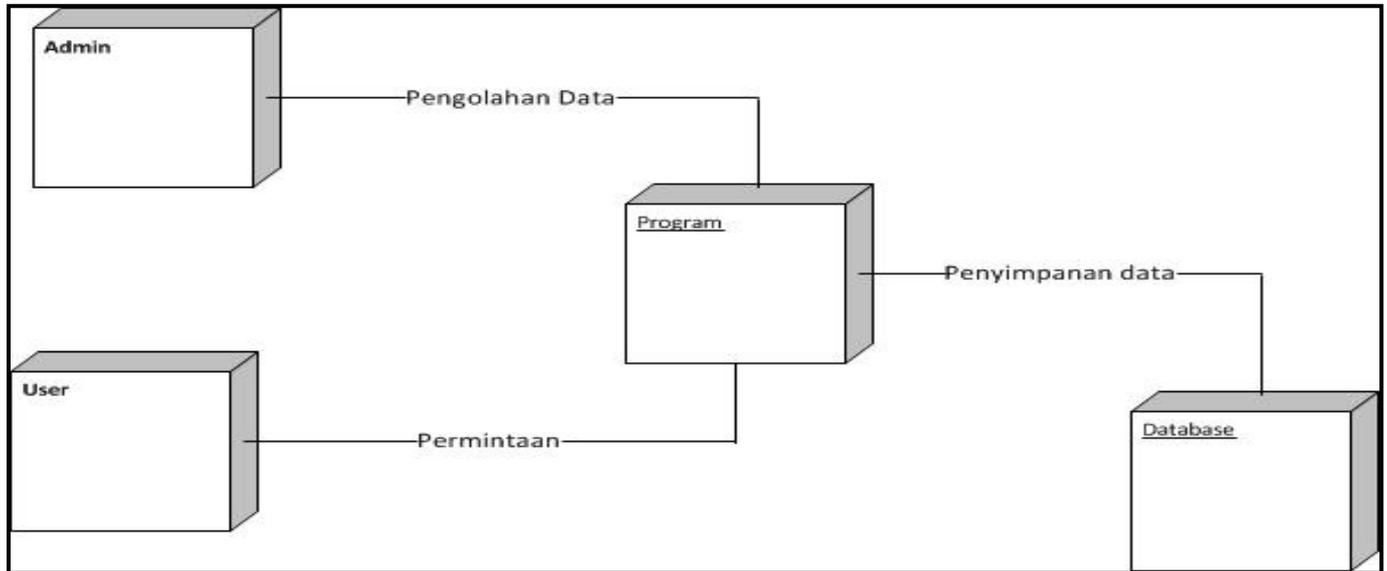


Sumber : Hasil penelitian (2014)

Gambar 8. *Sequence Diagram User* Pilih Kandidat

4. Deployment Diagram

Berikut adalah *Deployment Diagram* yang menggambarkan infrastruktur sistem *voting* bekerja.



Sumber : Hasil penelitian (2014)

Gambar 9. Deployment Diagram e-voting

E. Pseudo Code

Masalah utama dalam proses pembangkitan kunci adalah bagaimana menghasilkan kunci yang tidak dapat diprediksi. Ada berbagai metode yang dapat digunakan untuk menghasilkan sebuah bilangan prima yang besar. Tetapi sistem ini tidak menggunakan metode tersebut, melainkan bilangan prima tersebut diinput secara default ke dalam sistem.

1. Enkripsi.

Keamanan sistem *e-voting* pada user ditekankan pada pertanyaan keamanan yang mana telah dibuat saat pendataan calon pemilih oleh admin. Dan keamanan data seperti password telah di enkripsi. Algoritma enkripsi dalam sistem ini adalah sebagai berikut:

```

jumlah number := length(message);
type tampung is varray(20) of varchar2(20);
emp_tampung tampung := tampung();
tmp varchar2(3);
hitTmp NUMBER(1);
pesan varchar2(100);
BEGIN
emp_tampung.extend(jumlah);
FOR i IN 1..jumlah LOOP
tmp := null;
hitTmp := 0;
emp_tampung(i) := SUBSTR(message,i);
tmp := ASCII(emp_tampung(i));
hitTmp := LENGTH(tmp);

```

```

IF hitTmp = 2
THEN
tmp := '0' || tmp;
END IF;
pesan := pesan || tmp;
END LOOP;
RETURN pesan;

```

2. Dekripsi.

Penampilan pertanyaan keamanan yang telah di-enkripsi membutuhkan metode deskripsi atau kebalikan dari enkripsi yang berguna menterjemahkan data yang telah ter-enkripsi. Berikut adalah algoritma deskripsi:

```

jumlah INTEGER := LENGTH(message);
byk INTEGER;
hit_awal INTEGER := 1
type tmpType IS varray(10) of varchar2(10);
e_tmp tmpType := tmpType();
hasil VARCHAR2(50);
tmp VARCHAR2(1);
BEGIN
byk := jumlah/3;
e_tmp.extend(byk);
FOR i IN 1..byk LOOP
tmp := null;
e_tmp(i) := SUBSTR(message, hit_awal, 3);
tmp := CHR(e_tmp(i));
hasil := hasil || tmp;
hit_awal := hit_awal + 3;
END LOOP;
RETURN hasil;
END decod;

```

3. *Audit*

Semua perubahan data dan data yang dihapus telah di rekam oleh table audit dimana table audit bertujuan sebagai history yang merekam data lama dan mengadopsi sistem TRIGGER dari ORACLE berikut algoritma dari TRIGGER yang di adopsi oleh table audit:

TRIGGER audit

After update or delete on voting or kandidat or pemilih

For each row

Update audit

Tgl = sysdate, → ditetap kan tanggal di mana perubahan dilakukan

Data_ lama = :old.[fieldtabel], → data sebelum dirubah

F. User Interface

Interface program ini nanti nya akan terdiri dari beberapa form yang desainnya bisa di lihat sebagai berikut:

1. Desain Form Login.

header	
<div style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"> <p>User Name <input style="width: 100%;" type="text"/></p> <p>Password <input style="width: 100%;" type="password"/></p> <p style="text-align: center;"> <input type="button" value="Submit"/> <input type="button" value="Cancel"/> </p> </div>	
Footer	

Sumber : Hasil penelitian (2014)

Gambar 10. Desain Form Login

2. Desain Form Verifikasi Tanggal Lahir.

header	
Verifikasi tanggal lahir	
<p>Tanggal Lahir : <input style="width: 100%;" type="text"/></p> <p style="text-align: center;"> <input type="button" value="Submit"/> <input type="button" value="Cancel"/> </p>	
Footer	

Sumber : Hasil penelitian (2014)

Gambar 11. Desain Form Verifikasi Tanggal Lahir

3. Desain Form Pembuatan Pertanyaan Dan Jawaban Keamanan.

header	
Pertanyaan dan jawaban keamanan	
<p>Pertanyaan : <input style="width: 100%;" type="text"/></p> <p>Jawaban : <input style="width: 100%;" type="text"/></p> <p style="text-align: center;"> <input type="button" value="Submit"/> <input type="button" value="Cancel"/> </p>	
Footer	

Sumber : Hasil penelitian (2014)

Gambar 12. Desain Form Pembuatan Pertanyaan dan Jawaban Keamanan

4. Desain Form Utama

header	
Menu Bar	
Slider	
Content	
Footer	

Sumber : Hasil penelitian (2014)

Gambar 13. Desain Form utama

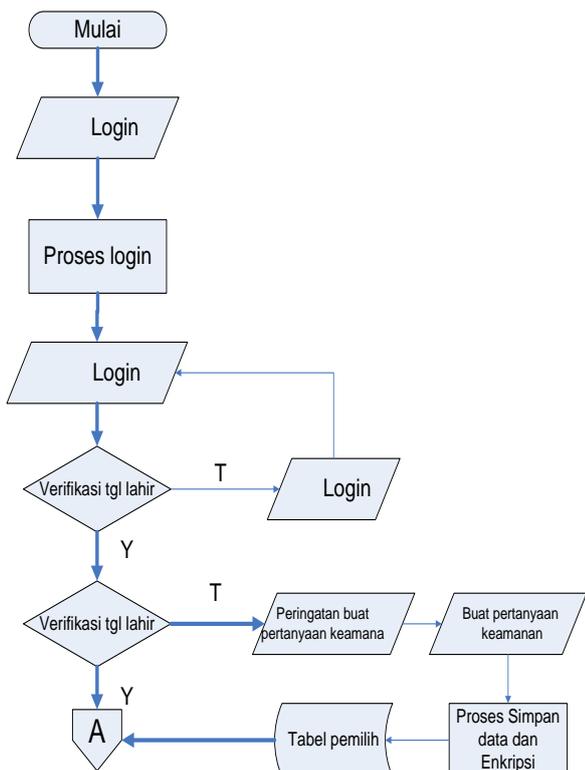
G. Implementasi

Rancangan *flowchart* merupakan rancangan alur proses yang ada dalam program

simulasi. Sistem *e-voting* ini mempunyai 2 keamanan yang pertama verifikasi tanggal lahir dan kedua pertanyaan keamanan yang mana pertanyaan keamanan dibuat secara privasi oleh pemilih pada waktu pertama kali login jika sudah menginputkan pertanyaan keamanan pemilih akan masuk ke menu utama.

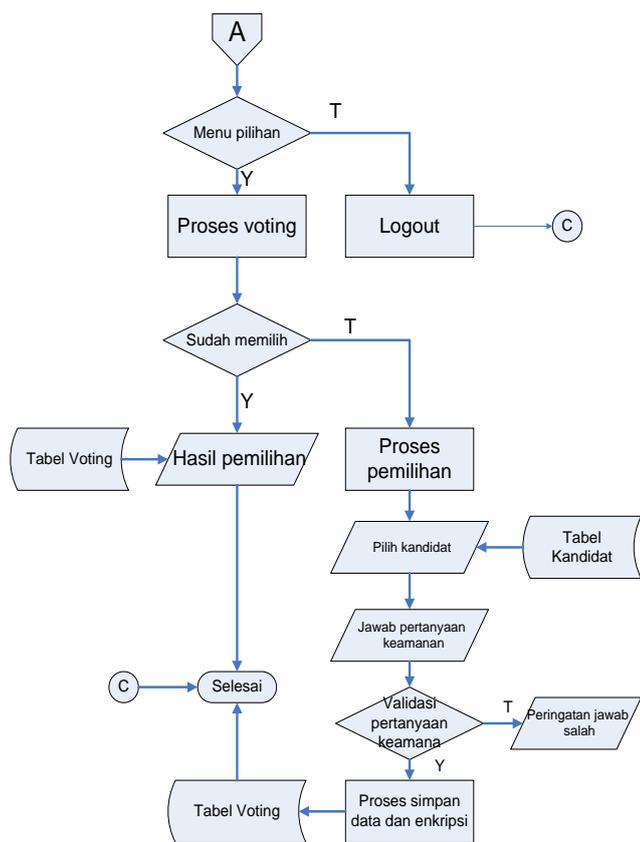
Password, pertanyaan keamanan beserta jawaban telah di enkripsi sehingga data tersebut bersifat privasi dan bertujuan untuk mengurangi resiko serangan berupa *snooping* atau *phising*. Menu utama dari *e-voting* berisi kan profil dari kandidat, hasil perolehan sementara, pemilahan (*voting*) dan logout.

Perolehan sementara dikemas dalam satu *procedure* yang bernama perhitungan sementara ini dimaksudkan untuk menjaga keamanan dari proses perhitungan dan memudahkan saat dipanggil ulang pada form admin. Seperti yang dijelaskan pada gambar berikut:



Sumber : Hasil penelitian (2014)

Gambar 14. Flowchart Voting Application



Sumber : Hasil penelitian (2014)

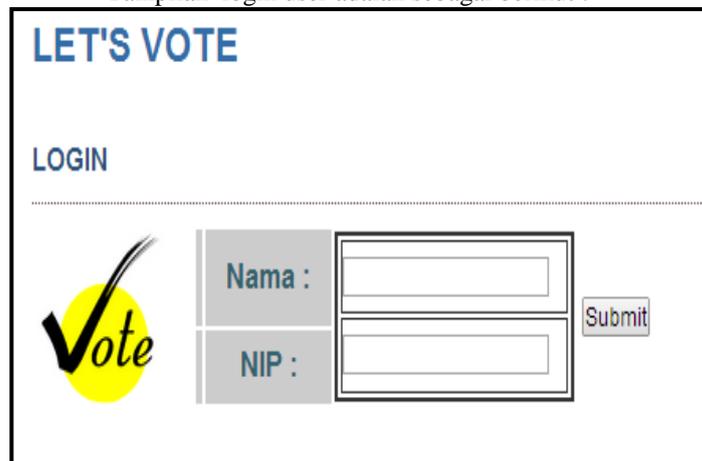
Gambar 15. Flowchart Voting Application

H. Testing

Testing dari perancangan sistem yang telah di jelaskan pada bab sebelumnya, serta bagaimana sistem di jalankan.

1. Login User

Tampilan login user adalah sebagai berikut :



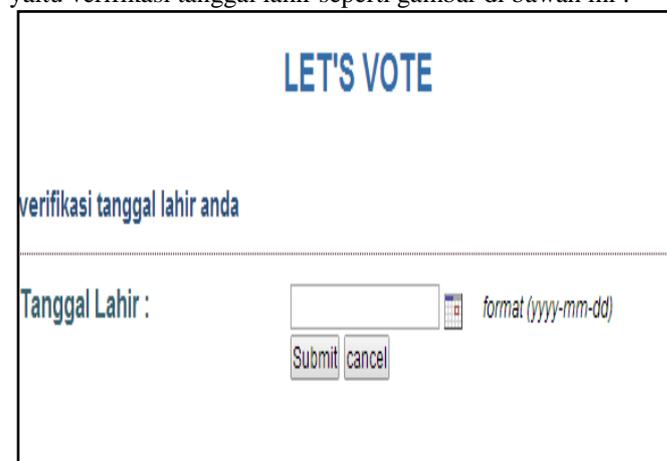
Sumber : Hasil penelitian (2014)

Gambar 16. Tampilan Login User

Dimana user yang telah di daftar akan login dengan menginputkan nama sebagai username dan NIP sebagai passwordnya.

2. Verifikasi tanggal lahir

User yang telah login dengan username dan password yang benar akan di alihkan ke halaman pengaman pertama yaitu verifikasi tanggal lahir seperti gambar di bawah ini :



Sumber : Hasil penelitian (2014)

Gambar 17. Halaman Verifikasi Tanggal Lahir

Tampilan di atas sama dengan password kedua dari user yang di ambil dari tanggal lahir tiap pemilih yang telah di enkripsi.

3. Halaman pembuatan pertanyaan dan jawaban keamanan

pembuatan pertanyaan keamanan pada pemilih yang telah berhasil login di gunakan untuk verifikasi pada saat proses pemilihan. Berikut adalah tampilan pembuatan pertanyaan dan jawaban keamanan :

Sumber : Hasil penelitian (2014)

Gambar 18. . Halaman Pembuatan Pertanyaan Dan Jawaban Keamanan

Pertanyaan dan jawabannya yang telah diinputkan nantinya akan di enkripsi demi keamanan hak pilih, berikut adalah hasil enkripsi dari pertanyaan dan jawaban pertanyaan di atas :

NIP	NAMA PEMILIH	ALAMAT PEMILIH	TGL_LHR	PERTANYAAN	JAWABAN	RES
1 048048052	Indro Susanto 2	Begalon, Panu...	1972-02-17	(null)	(null)	(null)
2 048048053	Ridwan Saupi	Pedurenan Mas...	1971-05-17	110097109097032097110097107063	122097104114097	100111110101
3 048048056	Sri Wahyono	Sragen, Jawa ...	1988-05-28	049043049	050	(null)
4 048048049	Prima Cop	Pisangan timo...	1991-09-16	049043049	050	100111110101
5 048048048	Hayu Ari	Halim perdana...	1992-02-24	049043049	050	(null)
6 048048055	Verri	Poltangan, Pa...	1987-01-12	049043049	050	100111110101
7 048048051	Yusup Bakrun	Miri, Sragen, ...	1975-05-06	050043050	052	100111110101
8 048048050	Fazri Stiyaning	Sukodadi, Lam...	1990-02-28	08709711411009703220710115117107097097110063	10910114097104	(null)
9 048048054	Dini Olivia	Depok jaya	1978-09-15	049043049	050	100111110101
10 048048057	Ganank Krisyanto	Semarang	1989-11-01	(null)	(null)	(null)

Sumber : Hasil penelitian (2014)

Gambar 19. Hasil Enkripsi Pertanyaan Dan Jawaban Keamanan

4. Halaman Utama User

Berikut adalah halaman utama pemilih :

Sumber : Hasil penelitian (2014)

Gambar 20. Halaman Utama User (Pemilih)

Halaman user (pemilih) berisi home sebagai halaman utama, voting sebagai halaman pemilihan yang muncul jika pemilih belum pernah memilih dan logout untuk keluar atau menghapus session.

5. Halaman pemilihan

User yang belum memilih berhak untuk memilih kandidat yang telah di daftarkan atau di calonkan. Seperti gambar berikut :

Sumber : Hasil penelitian (2014)

Gambar 21. Halaman Pemilihan (Voting)

Sumber : Hasil penelitian (2014)

Gambar 21. Halaman Pemilihan (Voting) Lihat Detail

6. Halaman pertanyaan keamanan setelah memilih

Halaman ini akan muncul sebagai sistem keamanan kedua setelah melakukan proses pemilihan.

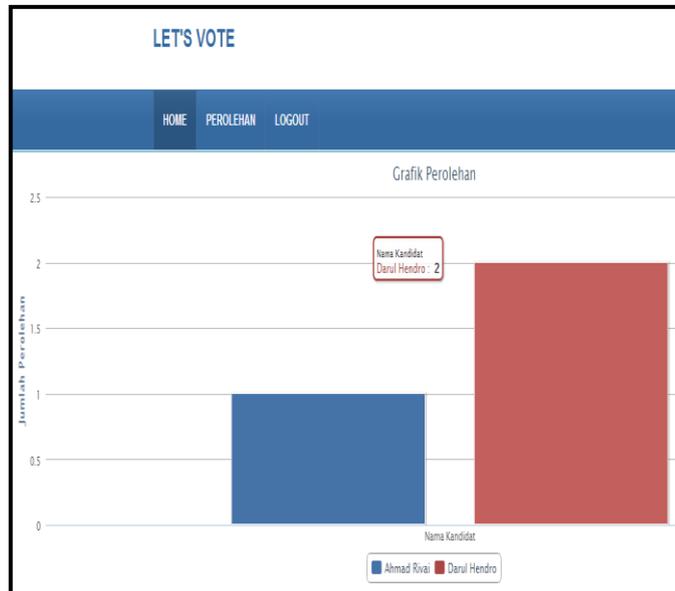
Sumber : Hasil penelitian (2014)

Gambar 22. Halaman Pertanyaan Keamanan

Pertanyaan yang telah di buat di depan oleh personal akan di munculkan sebagai sistem keamanan kedua setelah user memberikan hak pilihnya, jika terjadi kesalahan user akan di kembalikan untuk melakukan pemilihan ulang.

7. Halaman perolehan sementara

Setelah user melakukan proses pemilihan halaman voting akan di tutup dan diganti dengan halaman perolehan yang di tujukan untuk menghindari pengambilan suara ganda.



Sumber : Hasil penelitian (2014)

Gambar 23. Halaman Perolehan Sementara

Perolehan sementara hanya bisa di lihat setelah user memberikan hak pilih nya yang di tujukan agar pemilih tidak terpengaruhi oleh banyaknya suara pada masing-masing kandidat.

8. Halaman Login Admin

Sama hal nya dengan pemilih admin juga mempunyai halaman login sebagai berikut :

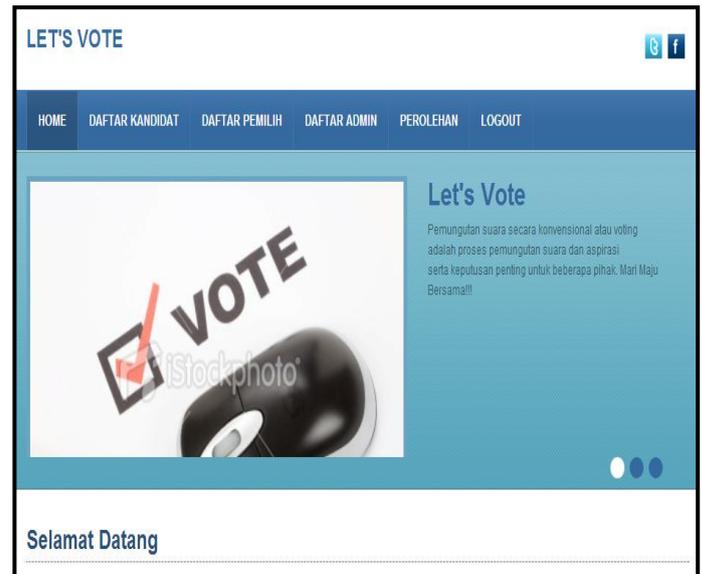
Sumber : Hasil penelitian (2014)

Gambar 24. Halaman Login Admin

Admin harus menggunakan id admin dan password yang di buat pada saat pendataan admin untuk bisa login ke halaman utama.

9. Halaman Utama Admin

Tampilan halaman utama admin adalah sebagai berikut :



Sumber : Hasil penelitian (2014)

Gambar 25. Halaman Utama Admin

Halaman utama admin berisi 4 tombol yang masing-masing mengarahkan ke halaman berbeda.

- Halaman daftar kandidat halaman ini dimaksudkan untuk pendaftaran kandidat admin.
- Halaman daftar pemilih halaman ini bertujuan untuk pendaftaran para pemilih oleh admin.
- Halaman daftar admin halaman ini memungkinkan untuk mendaftarkan admin baru.
- Halaman perolehan digunakan untuk memantau hasil perolehan sementara.

10. Halaman Pendaftaran Kandidat

Pendaftaran kandidat hanya bisa di lakukan oleh admin halaman pendaftaran kandidat adalah sebagai berikut :

KANDIDAT	
	<p>Nama : Ahmad Rivai</p> <p>Alamat : Pedurenan Masjid RT/RW 014/004 Karet kuningan, Stiabudi, Jakarta Selatan.</p> <p>Tanggal Lahir : 1982-02-27</p>
Prestasi	The Best Employee 2008-2011
visi misi	Visi: Terwujudnya organisasi pekerja yang senantiasa berjuang mewujudkan kesejahteraan lahir dan batin kaum pekerja dan keluarganya melalui hubungan kerja yang harmonis dan berkeadilan dalam Negara Republik Indonesia yang demokratis, berdaulat dalam lindungan Tuhan Yang Maha Esa. Misi: Mewujudkan tata kelola ketenagakerjaan yang baik dan bersih, melindungi segenap Bangsa Indonesia, mewujudkan kesejahteraan umum serta mencerdaskan kehidupan bangsa Indonesia memajukan kesejahteraan umum serta mencerdaskan kehidupan bangsa.

Sumber : Hasil penelitian (2014)

Gambar 26. Halaman Pendaftaran Kandidat

Halaman ini digunakan saat proses pendaftaran pemilih oleh admin. Yang nantinya NIP pemilih akan di enkripsi jika inputan "001" menghasilkan output sebagai berikut :

NIP	NAMA PEMILIH	ALAMAT PEMILIH	TGL_LHR
1 048048052	Indro Susanto	Begalon, Panularan, Laweyan, Surakarta	1972-02-17
2 048048053	Ridwan Sauqi	Pedurenan Masjid III	1971-05-17
3 048048056	Sri Wahyono	Sragen, Jawa Tengah	1988-05-28
4 048048049	Prima Cop	Pisangan timur, Pulogadung, Jakarta Timur.	1991-09-16

Sumber : Hasil penelitian (2014)

Gambar 27. Hasil Enkripsi NIP

Penambahan admin di tujuan untuk penambahan admin baru yang akan membantu kinerja admin-admin lain. Dimana password akan di enkripsi sebagai berikut :

ID_ADMIN	NAMA_ADMIN	ALAMAT_ADMIN	PASSWORD
1 001	aik	surabaya	097105107111

Sumber : Hasil penelitian (2014)

Gambar 28. Hasil Enkripsi Password Admin

V.KESIMPULAN

Berdasarkan pembahasan di atas dapat diambil kesimpulan antara lain :

1. *E-voting* menjadi alternatif proses pemungutan suara yang lebih mudah dan cepat serta dapat menurunkan tingkat kesalahan. Walaupun penerapan *e-voting* menyisakan persoalan terkait soal keamanan informasi yaitu keutuhan data (*integrity*), kerahasiaan informasi (*confidentiality*), dan ketersediaan informasi (*availability*).

2. Enkripsi dapat dimanfaatkan untuk menjawab pertanyaan terkait dengan keamanan informasi berupa kerahasiaan, keutuhan data, nir penyangkalan, serta otentikasi.
3. Sistem *e-voting* berbasis web menggunakan bahasa pemrograman PHP dan database Oracle dan menunjukkan bahwa algoritma kode ASCII cukup aman digunakan untuk keamanan informasi pada e-voting.

REFERENSI

- [1] Adnan. Metode Devide and Conquer Parallel dan Parallel-Reduce Pada Cilk for Untuk Aplikasi E-Voting Berbasis Sistem Prosesor Multicore. Makassar: Seminar Nasional Aplikasi Teknologi Informasi ISSN: 1907-5022 15 Juni 2014.
- [2] Al fatah, Hanif. Analisis dan perancangan system Informasi untuk keunggulan bersaing di perusahaan dan organisasi Modern. Yogyakarta: Andi. 2007.
- [3] Dharwiyanti, S dan Wahono, S.R. Pengantar Unified Modeling Language. www.Ilmukomputer .com. (20 Juli 2014). 2003.
- [4] Hutagalung, Kifki Muhammad. Perancangan Perangkat E-Voting E-KTP. Medan: Jurnal Saintikom Vol. 11, No.1 Januari 2012: 48-56. 2012.
- [5] Rafiudin, rahmat. Sistem Komunikasi Data Mutakhir: Yogyakarta : Andi. 2006.
- [6] Rosa a.s dan M.salahudin. Rekayasa perangkat lunak terstruktur dan berorientasi objek. Bandung: informatika. 2014.
- [7] Yasin, Verdi. Rekayasa Perangkat lunak Berorientasi Objek. Jakarta: Mitra Wacana Media. . 2012.



Prima cop.. Tahun 2014 lulus dari Program Strata Satu (S1) Program Studi Sistem Informasi STMIK Nusa Mandiri Jakarta.



Rachmat Adi Purnama M.Kom. Tahun 1997 lulus dari Program Strata Satu (S1) Program Studi Sistem Informasi STMIK BUDI LUHUR Jakarta. Tahun 2010 lulus dari Program Strata Dua (S2) Program Pascasarjana Magister Ilmu Komputer STMIK Nusa Mandiri Jakarta. Tahun 2011 sudah tersertifikasi dosen dengan Jabatan Fungsional Akademik Lektor di AMIK BSI Jakarta..